

CLAIMS

1. A computer system for receiving encrypted compressed content and for producing decrypted decompressed content based on the received encrypted compressed content, the system comprising:

a decryption element for decrypting the content based at least in part on a content key; and

a decompression element for decompressing the content based at least in part on the content key,

wherein the content key is employed to decrypt the content and also to decompress the content.

2. The computer system of claim 1 comprising:

a decryption element having an input for receiving the encrypted compressed content, the decryption element for decrypting the encrypted compressed content based at least in part on a content key to result in decrypted compressed content, and having an output for producing the decrypted compressed content; and

a decompression element having an input for receiving the decrypted compressed content, the decompression element for decompressing the decrypted compressed content based at least in part on the content key to result in decrypted decompressed content, and having an output for producing the decrypted decompressed content,

wherein a content thief that obtains the decrypted compressed content from the output of the decryption element cannot decompress the obtained decrypted compressed content by way of another decompression element without the content key.

3. The computer system of claim 1 wherein the decompression element has a number of adjustable parameters and wherein the decompression element employs the content key as at least one of the adjustable parameters.

4. The computer system of claim 3 wherein the decompression element includes an internal representation having DCT coefficients of macroblocks, and wherein the coefficients are de-scrambled and de-noised according to the content key.

5. The computer system of claim 3 wherein the decompression element includes a quantizer for performing a lossy quantization step, and wherein the quantizer is de-dithered according to the content key.

6. The computer system of claim 1 wherein the decryption element supplies the content key to the decompression element.

7. The computer system of claim 1 wherein the decompression element includes the decryption element.

8. The computer system of claim 1 wherein the decryption element includes the decompression element.

9. A computer system for receiving content and for producing encrypted compressed content based on the received content, the system comprising:

an encryption element for encrypting the content based at least in part on a content key; and

a compression element for compressing the content based at least in part on the content key,

wherein the content key is employed to encrypt the content and also to compress the content.

10. The computer system of claim 9 comprising:
a compression element having an input for receiving the content, the compression element for compressing the content based at least in part on a content key to result in compressed content, and having an output for producing the compressed content; and

an encryption element having an input for receiving the compressed content, the encryption element for encrypting the compressed content based at least in part on the content key to result in encrypted compressed content, and having an output for producing the encrypted compressed content,

wherein the encrypted compressed content from the output of the encryption element cannot be decompress without the content key.

11. The computer system of claim 9 wherein the compression element has a number of adjustable parameters and wherein the compression element employs the content key as at least one of the adjustable parameters.

12. The computer system of claim 11 wherein the compression element includes an internal representation having DCT coefficients of macroblocks, and wherein the coefficients are scrambled and noised according to the content key.

13. The computer system of claim 11 wherein the compression element includes a quantizer for performing a lossy quantization step, and wherein the quantizer is dithered according to the content key.

14. A method for receiving encrypted compressed content and for producing decrypted decompressed content based on the received encrypted compressed content, the method comprising:

decrypting the content based at least in part on a content key;
and
decompressing the content based at least in part on the
content key,
wherein the content key is employed to decrypt the content and also
to decompress the content.

15. The method of claim 14 comprising:
decrypting the encrypted compressed content based at least
in part on a content key to result in decrypted compressed content; and
decompressing the decrypted compressed content based at
least in part on the content key to result in decrypted decompressed content,
wherein a content thief that obtains the decrypted compressed
content cannot decompress the obtained decrypted compressed content without
the content key.

16. The method of claim 14 wherein decompression is based on
a number of adjustable parameters and wherein decompression comprises
employing the content key as at least one of the adjustable parameters.

17. The method of claim 16 wherein decompression is based on
an internal representation having DCT coefficients of macroblocks, and wherein
decompression comprises de-scrambling and de-noising the coefficients
according to the content key.

18. The method of claim 16 wherein decompression is based on
a quantizer for performing a lossy quantization step, and wherein decompression
comprises de-dithering the quantizer according to the content key.

19. A method for receiving content and for producing encrypted
compressed content based on the received content, the method comprising:

encrypting the content based at least in part on a content key;
and
compressing the content based at least in part on the content
key,
wherein the content key is employed to encrypt the content and also
to compress the content.

20. The method of claim 19 comprising:
compressing the content based at least in part on a content
key to result in compressed content; and
encrypting the compressed content based at least in part on
the content key to result in encrypted compressed content,
wherein the encrypted compressed content from the output of the
encryption element cannot be decompress without the content key.

21. The method of claim 19 wherein compression is based on a
number of adjustable parameters and wherein compression comprises employing
the content key as at least one of the adjustable parameters.

22. The system of claim 21 wherein compression is based on an
internal representation having DCT coefficients of macroblocks, and wherein
compression comprises scrambling and noising the coefficients according to the
content key.

23. The system of claim 21 wherein compression is based on a
quantizer for performing a lossy quantization step, and wherein compression
comprises dithering the quantizer according to the content key.

24. A computer-readable medium having computer-executable
instructions thereon for receiving encrypted compressed content and for producing

decrypted decompressed content based on the received encrypted compressed content, the instructions being organized into modules including:

a first module for decrypting the content based at least in part on a content key; and

a second module for decompressing the content based at least in part on the content key,

wherein the content key is employed to decrypt the content and also to decompress the content.

25. The medium of claim 24 comprising:

a first module for decrypting the encrypted compressed content based at least in part on a content key to result in decrypted compressed content; and

a second module for decompressing the decrypted compressed content based at least in part on the content key to result in decrypted decompressed content,

wherein a content thief that obtains the decrypted compressed content cannot decompress the obtained decrypted compressed content without the content key.

26. The medium of claim 24 wherein the second module

decompresses based on a number of adjustable parameters and wherein the second module employs the content key as at least one of the adjustable parameters.

27. The medium of claim 26 wherein the second module

decompresses based on an internal representation having DCT coefficients of macroblocks, and wherein the second module de-scrambles and de-noises the coefficients according to the content key.

28. The medium of claim 26 wherein the second module decompresses is based on a quantizer for performing a lossy quantization step, and wherein the second module de-dithers the quantizer according to the content key.

29. A computer-readable medium having computer-executable instructions thereon for receiving content and for producing encrypted compressed content based on the received content, the method comprising:

a first module for encrypting the content based at least in part on a content key; and

a second module for compressing the content based at least in part on the content key,

wherein the content key is employed to encrypt the content and also to compress the content.

30. The medium of claim 29 comprising:

a first module for compressing the content based at least in part on a content key to result in compressed content; and

a second module for encrypting the compressed content based at least in part on the content key to result in encrypted compressed content,

wherein the encrypted compressed content from the output of the encryption element cannot be decompress without the content key.

31. The medium of claim 29 wherein the first module compresses based on a number of adjustable parameters and wherein the first module employs the content key as at least one of the adjustable parameters.

32. The system of claim 31 wherein the first module compresses based on an internal representation having DCT coefficients of macroblocks, and

wherein the first module scrambles and noises the coefficients according to the content key.

33. The system of claim 31 wherein the first module compresses based on a quantizer for performing a lossy quantization step, and wherein the first module dithers the quantizer according to the content key.

2025-03-03 14:00:00